A

EXAM OBJECTIVES FOR MCSE CERTIFICATION EXAM #70-220: DESIGNING SECURITY FOR A MICROSOFT WINDOWS 2000 NETWORK

ANALYZING BUSINESS REQUIREMENTS

Objective	Chapter: Section	Hands-on Project(s)
Analyze the existing and planned business models. ■ Analyze the company model and the geographical scope. Models include regional, national, international, subsidiary, and branch offices. ■ Analyze company processes. Processes include information flow, communication flow, service and product life cycles, and decision-making.	Chapter 2: Identifying Business Models	
Analyze the existing and planned organizational structures. Considerations include management model; company organization; vendor, partner, and customer relationships; and acquisition plans.	Chapter 2: Identifying Business Models	
Analyze factors that influence company strategies. ■ Identify company priorities. ■ Identify the projected growth and growth strategy. ■ Identify relevant laws and regulations. ■ Identify the company's tolerance for risk. ■ Identify the total cost of operations.	Chapter 2: Identifying Corporate Strategies and Goals	

Objective	Chapter: Section	Hands-on Project(s)
Analyze business and security requirements for the end user.	Chapter 2: Identifying the Current Security Model	
Analyze the structure of IT management. Considerations include type of administration, such as centralized or decentralized; funding model; outsourcing; decision-making process; and change-management process.	Chapter 2: Identifying IT Administrative Structures	
Analyze the current physical model and information security model. ■ Analyze internal and external security risks.	Chapter 2: Identifying the Current Technical Environment Chapter 1: Internal Security Risks Chapter 1: External Security Risks	

ANALYZING TECHNICAL REQUIREMENTS

Objective	Chapter: Section	Hands-on Project(s)
Evaluate the company's existing and planned technical environment. ■ Analyze company size and user and resource distribution. ■ Assess the available connectivity between the geographic location of work sites and remote sites. ■ Assess the net available bandwidth. ■ Analyze performance requirements. ■ Analyze the method of accessing data and systems. ■ Analyze network roles and responsibilities. Roles include administrative, user, service, resource ownership, and application.	Chapter 2: Identifying the Current Technical Environment	
Analyze the impact of the security design on the existing and planned technical environment. ■ Assess existing systems and applications. ■ Identify existing and planned upgrades and rollouts. ■ Analyze technical support structure. ■ Analyze existing and planned network and systems management.	Chapter 1: Managing Security Risks Chapter 2: Identifying the Current Technical Environment	

ANALYZING SECURITY REQUIREMENTS

Objective	Chapter: Section	Hands-on Project(s)
Design a security baseline for a Windows 2000 network that includes domain controllers, operations masters, application servers, file and print servers, RAS servers, desktop computers, portable computers, and kiosks.	Chapter 4: Securing Active Directory Chapter 6: Securing Servers Using Security Templates	Project 4-1 Project 4-2 Project 4-3 Project 4-4 Project 4-5
Identify the required level of security for each resource. Resources include printers, files, shares, Internet access, and dial-in access.	Chapter 3: All sections Chapter 6: All sections	Project 3-1 Project 3-2 Project 3-3 Project 3-4

DESIGNING A WINDOWS 2000 SECURITY SOLUTION

Objective	Chapter: Section	Hands-on Project(s)
Design an audit policy.	Chapter 3: Configuring an Audit Policy	Project 3-6 Project 3-7
Design a delegation of authority strategy.	Chapter 4: Delegating Administrative Tasks	Project 4-6
Design the placement and inheritance of security policies for sites, domains, and organizational units.	Chapter 4: Implementing Group Policies for Security	Project 4-8
Design an Encrypting File System strategy.	Chapter 3: Encrypting File System	Project 3-5
Design an authentication strategy. ■ Select authentication methods. Methods include certificate-based authentication, Kerberos authentication, clear-text passwords, digest authentication, smart cards, NTLM, RADIUS, and SSL. ■ Design an authentication strategy for integration with other systems.	Chapter 3: Implementing User Authentication Chapter 6: Implementing Secure Access for Non-Microsoft Clients	
Design a security group strategy.	Chapter 4: Implementing Security Groups	Project 4-7
Design a Public Key Infrastructure. ■ Design Certificate Authority (CA) hierarchies. ■ Identify certificate server roles. ■ Manage certificates. ■ Integrate with third-party CAs. ■ Map certificates.	Chapter 5: All sections	Project 5-1 Project 5-2 Project 5-3 Project 5-4

Objective	Chapter: Section	Hands-on Project(s)
Design Windows 2000 network services security. ■ Design Windows 2000 DNS security. ■ Design Windows 2000 Remote Installation Services (RIS) security. ■ Design Windows 2000 SNMP security. ■ Design Windows 2000 Terminal Services security.	Chapter 6: All sections	Project 6-1 Project 6-2 Project 6-3 Project 6-4 Project 6-5

DESIGNING A SECURITY SOLUTION FOR ACCESS BETWEEN NETWORKS

Objective	Chapter: Section	Hands-on Project(s)
Provide secure access to public networks from a private network.	Chapter 10: Securing User Access to the Internet	Project 10-1 Project 10-2 Project 10-3 Project 10-4
Provide external users with secure access to private network resources.	Chapter 10: Securing the Internal Network from the Internet	
Provide secure access between private networks. ■ Provide secure access within a LAN. ■ Provide secure access within a WAN. ■ Provide secure access across a public network.	Chapter 9: All sections	Project 9-1 Project 9-2 Project 9-3 Project 9-4
Design Windows 2000 Security for remote access users.	Chapter 8: All sections	Project 8-1 Project 8-2 Project 8-3 Project 8-4

DESIGNING SECURITY FOR COMMUNICATION CHANNELS

A

Objective	Chapter: Section	Hands-on Project(s)
Design an SMB-signing solution.	Chapter 7: Implementing Server Message Block Signing	Project 7-1
Design an IPSec solution. ■ Design an IPSec encryption scheme. ■ Design an IPSec management strategy. ■ Design negotiation policies. ■ Design security policies. ■ Design IP filters. ■ Define security levels.	Chapter 7: Securing Network Traffic Using IPSecurity	Project 7-2 Project 7-3 Project 7-4